



“Defensive Battle Stations In Network- Centric Warfare: Rapid- Response Cyber Forensics™”

Stephen B. Webb

**Lockheed Martin
Mission Systems**

**J. Philip Craiger, Ph.D
at Omaha**

University of Nebraska



What Is Rapid-Response Cyber Forensics™ ?

- **Rapid-Response Cyber Forensics™ is an approach to the defense of critical military computers and networks.**
- **It augments “live” computer defense with skilled cyber forensic practitioners and adds a new element to defense-in-depth of critical automated systems.**



What Rapid-Response Cyber Forensics™ Is NOT

- **RRCF is NOT a substitute or replacement for any security tools or procedures being used on your systems today.**
- **RRCF is NOT a “fire-and-forget silver bullet” which will magically solve all your defensive network concerns.**



LM-MS and PKI Partnership

- **An uncommon partnership between Academics and Business with a common goal:**

“Field the Best Military Cyber-Defenders in the World”
- **Leverage the strengths of both LM-MS and PKI to create a product neither could build alone**



Benefits of Partnership

- **LM-MS wanted to provide security training for our Government client**
 - *We knew what training could be valuable, but were not in the training business*
- **PKI wanted to expand into this area, but lacked experience with a military client**
 - *They knew how to train, but not what to train*
- **Both partners shared a strong desire to make the partnership work**



Stones on the Path to Success

- **Non-congruent Initial Goals**
- **Culture Clash**
- **Lack of Process**



Network-Centric Landscape

- **The U.S. holds a decisive edge in Network-Centric Warfare**
 - *Asymmetric threats are emerging to challenge our pre-eminence*
- **Our combatant networked systems must be defended to assure information superiority and victory**
 - *Tools for network defense are rapidly superceded by ever-more-virulent attacks*
- **Nothing we are proposing replaces any of the defensive tools presently being used**



Network-Centric Warfare

- As conflict in Iraq demonstrated, Network-Centric Warfare gives a Commander a decisive advantage against any adversary—this point is not lost on our future enemies
- The nature of network attack will continue to be appealing to those enemies as an “equalizer”
 - *low cost*
 - *technologically simple*
 - *effective, low profile, and low risk of attribution*
- Rapid response to attacks against our network-centric forces will be necessary for military commanders to sustain future operations



The Network-Centric Commander

- A successful military commander in the 21st century must “detect, diagnose, and decide”—then act—against varying types and sources of cyber-attacks
- A Network-Centric Commander must sustain network operations while under computer network attack
- Tools and procedures for doing this have analogues in the non-military world, typically called cyber forensics
 - “Classic” cyber forensics: acquiring and authenticating evidence, analyzing that evidence for evidentiary value, and presenting the results in a court of law
 - These classic tools and procedures are ill-suited for a commander under attack



Cyber Forensic Practice

- **Analysis after the fact—the “medical examiner” model**
 - *A law enforcement mind set*
 - Post hoc analysis
 - Duplicate evidence, verify authenticity, offline analysis
- **Focus of present cyber forensic training**
- **Defensive and conservative, it has served law enforcement well, but fails to meet the needs of a commander for sustained operations under cyber attack**
 - *Critical information repositories must remain online*
 - *Live-response is the key*



Rapid Response

- **We propose a rapid response cyber forensic approach more resembling an Emergency Medical Technician than a Medical Examiner**
- **Tools, protocols, and techniques to perform “cyber-triage”**
 - *evaluating, prioritizing and defending against attacks against our war fighting networks*
 - *intelligent application of tools and procedures applicable to the warfighting context*



Warfighting Cyber Forensics

- **Development of new cyber forensic tools is a key component of rapid-response forensics, and while crucial, is not the primary focus of our efforts**
- **A disciplined cadre of cyber forensic technicians will remain the key to success in defending warfighting systems**
 - *Live response to sustain operations*
- **Expert cyber-triage of multiple and simultaneous attacks**



Rapid-Response Cyber Forensics™

- **Developed collaboratively between University of Nebraska at Omaha and Lockheed Martin Mission Systems**
 - ***An alternative to traditional law-enforcement-like response***
 - “Classic” forensics not suited to dynamic, real-time warfighting environment
 - ***Both a human-capital and technological solution***
- **Success depends upon a fusion of procedures, techniques, and practice**



Three Foundations of RRCF



- **Training tailored for RRCF practitioners**
- **Procedures for forensic examination of “live” computer systems in real time**
- **Regular team practice in a lab environment mirroring real-world threats**



Training as Key Component

- **Practitioners receive rigorous hands-on initial training in RRCF techniques with realistic examples**
- **Training combines a deep understanding of:**
 - *Techniques and technologies*
 - *Realistic hands-on scenario-based practice*
- **As technology changes, rapid-response cyber forensics™ practitioners skills are reinforced and upgraded**



Rapid-Response Skill Set

- **Understanding of Technology**
 - *Networks: protocols, attack signatures, normal & abnormal network traffic*
 - *Kept current through training*
- **Analytical Skills**
 - *Recognition and understanding of threats*
 - *Refined through practice in the lab*
- **Tools**
 - *Employment of the right tool—at the right time*



Procedure and Drill

- **Inter-related: Procedures are complex, and make drill central to proficiency**
 - *Development of detailed procedures*
 - *Application of the correct procedure to counter threats*
- **Practice when (or “if”) a procedure should be used**
 - *achieved in a lab setting where virulent attacks may be staged without risk to actual systems*



Results

- **Two classes of RRCF practitioners trained**
 - *Screening with a pre-test identified good candidates*
 - *All students successfully certified in RRCF*
- **Excellent customer response**
- **Plans for expanding the program**



Lessons Learned

- **A partnership between Business and Academics must serve the goals of both**
 - *Expect some surprises*
- **Rapid-Response Cyber Forensics™ is feasible**
 - *It is possible to achieve effectiveness—affordably*
 - *Training was challenging, but successfully scaled to the target audience*
 - *Importance of appropriate skill set in students*



The Future of Rapid-Response Cyber Forensics™

- **As technology and tools change, so must the RRCF practitioner**
 - *Ongoing refresher training using realistic hands-on simulations and exercises*
- **Adopt and adapt new cyber forensic techniques that are developed**
 - *Requires continuing education on the part of cyber forensic trainers*
- **Develop new cyber forensic procedures in concert with new network-centric warfighting capabilities**



Contact Information

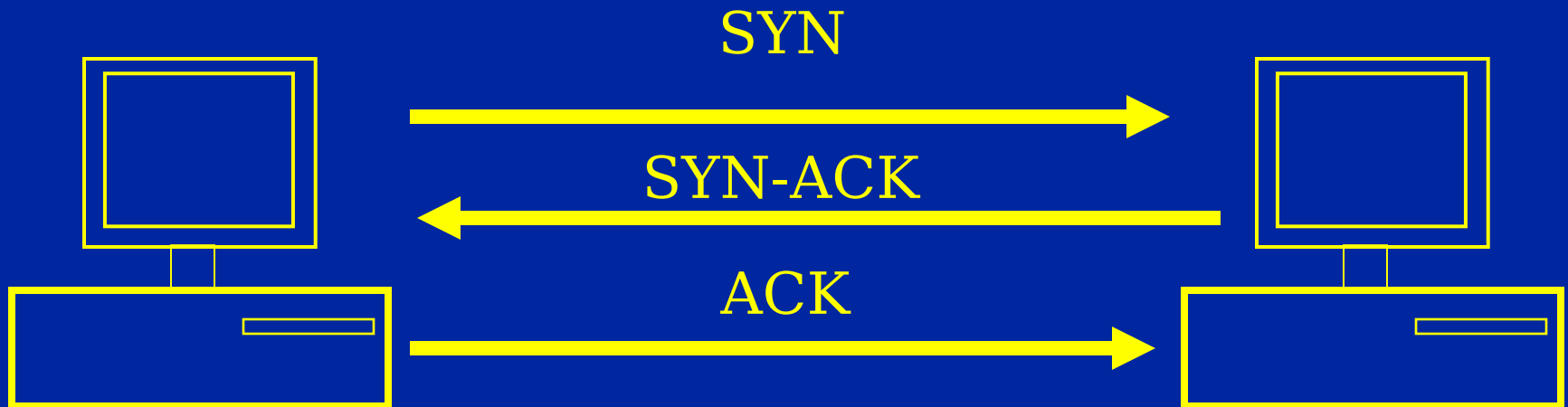
- **E-mail**
 - *stephen.b.webb@lmco.com*
 - *philip_craiger@unomaha.edu*
- **We'd be pleased to answer your questions**
- **Thank you**



Back-Up Slides



Starting a Computer Conversation



- **Final ACK completes the connection.**
- **Computers now have a reliable channel for communication**



Computer Dialog

```
[1] 10:51:18.097489 whammo.cobalt.net.33593 > server1.unomaha.edu.ftp S
4022300050:4022300050(0) win 58 40 <mss 1460> (DF)

[2] 10:51:18.115166 server1.unomaha.edu.ftp > whammo.cobalt.net.33593 S
1161910619:1161910619(0) ack 40 22300051 win 17520 <mss 1460> (DF)

[3] 10:51:18.115218 whammo.cobalt.net.33593 > server1.unomaha.edu.ftp: .ack 1
win 5840 (DF)
```

- This is an example of a normal “handshake” between two computers
 - *whammo.cobalt.net asks to connect, s=“syn”, a request to synchronize*
 - *Server1.unomaha.edu answers “syn-ack”, to acknowledge*
 - *whammo.cobalt.net sends a final “ack” and establishes connection*



Normal Traffic?

```
[1] 10:51:18.097489 192.168.100.105.33593 > server1.unomaha.edu.netbios-ssn S
4022300050:4022300050(0) win 58 40 <mss 1460> (DF)

[2] 10:51:18.115218 192.168.100.104.33594 > server1.unomaha.edu.netbios-ssn S
4022300051:4022300051(0) win 58 40 <mss 1460> (DF)

[3] 10:51:18.097489 192.168.100.107.33595 > server1.unomaha.edu.netbios-ssn S
4022300052:4022300052(0) win 58 40 <mss 1460> (DF)

[4] 10:51:18.115218 192.168.100.105.33596 > server1.unomaha.edu.netbios-ssn S
4022300053:4022300053(0) win 58 40 <mss 1460> (DF)

[5] 10:51:18.097489 192.168.100.111.33597 > server1.unomaha.edu.netbios-ssn S
4022300054:4022300054(0) win 58 40 <mss 1460> (DF)
```



SYN-Attack



- **There is no final ACK**
- **Connection is never established**
- **2nd Computer ends up using all of its resources waiting for the final ACK**



End

- **Thank you**